I CLAIM:

1. In a computer system connected to an external communications medium,a security device comprising:

a programmable firewall device interposed between the computer system and the external communications medium;

a controller device configured within the computer system such that said controller device can access all communications into and out of the computer system; and

a communications device for communicating instructions from said controller device to ~~said firewall device for controlling said firewall device.~~

2. The computer system of claim 1, wherein:
the computer system is a local area network.

3. The computer system of claim 1, wherein:
the external communications medium is the internet.

4. The computer system of claim 1, wherein:
the computer system is a local area network operating as an Ethernet network.

5. The computer system of claim 1, wherein:
the controller device examines communications incoming to the computer system for code known to be associated with attempted security breaches.

6. The computer system of claim 1, wherein:

the controller device examines communications incoming to the computer system for patterns of activity indicative of attempted security breaches.

7. The computer system of claim 1, wherein:

the controller device controls the firewall to block communications between the computer system and the external communications medium when an attempted security breach is detected.

8. The computer system of claim 1, wherein:

the communications device is a serial data communications link.

9. The computer system of claim 1, wherein:

the controller assigns a value to a perceived attempted security breach;

and the controller controls the firewall to block communications between the computer system and the external communications medium for a predetermined period according to the value assigned to the perceived attempted security breach.

10. The computer system of claim 1, wherein:

the controller assigns a value to a perceived attempted security breach;

and the controller controls the firewall to block communications between a selected portion of the computer system and the external communications medium according to the value assigned to the perceived attempted security breach.

11. The computer system of claim 1, wherein:

the controller is a general purpose computer programmed to function as described in claim 1.

12. The computer system of claim 1, wherein:

the controller and the firewall are each physically distinct computerized units.

13. In a local area network attached to a wide area network, a method for improving the security of the local area network, comprising:

16

monitoring communications between the local area network and the wide area network;

determining, over time, if the communications between the local area network and the wide area network contain patterns of activity indicative of an attempted security breach; and

controlling a firewall to selectively block communications between the local area network and the wide area network depending upon a classification of the attempted security breach.

13 ~~14~~. The method of claim 12 ~~13~~, wherein:

the wide area network is the internet.

14 ~~15~~. The method of claim 12 ~~13~~, wherein:

the local area network is an Ethernet local area network.

15 ~~16~~. The method of claim 12 ~~13~~, wherein:

the classification of the attempted security breach includes a factor relating to the importance of a portion of the local area network which the attempted security breach attempts to access.

16 ~~17~~. The method of claim 12 ~~13~~, wherein:

the classification of the attempted security breach includes a factor relating to the number of attempts made in the course of the attempted security breach.

17 ~~18~~. The method of claim 12 ~~13~~, wherein:

the classification of the attempted security breach includes a factor relating to the relative sophistication of the attempted security breach.

18 ~~19~~. The method of claim 12 ~~13~~, wherein:

the classification of the attempted security breach is accomplished by a controller unit which is physically distinct from a firewall unit.

19 ~~20~~. The method of claim 18 ~~19~~, wherein:

the firewall unit is controlled through a serial datalink from the controller unit.

21. A computer program product comprising a computer usable medium having a computer readable code embodied thereon configured to operate on a computer, comprising:

a detect code operation wherein known improper code is detected; and

a detect patterns operational routine wherein a pattern of activity is detected over time.

22. The computer program product of claim 21, and further including:

a weighting operation wherein a weight is assigned to a detected security breach.

23. The computer program product of claim 21, wherein:

a firewall is automatically reprogrammed.

24. A computer program product comprising a computer usable medium having a computer readable code embodied thereon configured to operate on a computer, comprising:

at least one detect operation wherein a computer security breach is detected; and

a weighting operation wherein a weight is assigned according to the importance of the security breach.

25. The computer program product of claim 24, and further including:

a react operation wherein a firewall is reprogrammed in real time to react to the security breach.

26. A computer program product comprising a computer usable medium having a computer readable code embodied thereon configured to operate on a computer, comprising:

at least one detect operation wherein a computer security breach is detected; and

a react operation wherein a firewall is reprogrammed in real time to react to the security breach.

27. The computer program product of claim 26, wherein:

said react operation reprograms the firewall according to an assigned weight, the assigned weight being a function of the type of security breach detected.